CyberGenerations Workshop

Facilitator Guide

This document provides instructions to Facilitators on how to effectively deliver a CyberGenerations workshop. It informs Facilitators how to prepare, what to prepare, and what to say and do to facilitate the lessons effectively.

Table of Contents

About this Workshop

Workshop Overview

- This workshop is made available through the generous support of AT&T and references information and resources available on AT&T’s Cyber Aware site.
- The goal of CyberGenerations is to equip senior citizens with an introductory understanding of how to keep themselves and their devices protected from various scams and cyber threats.
- This is not a general computer education course. The curriculum is a guide for people who are semi- or fully active online. The material primarily teaches cyber hygiene and scam awareness.
- Though the topics discussed are universally relevant, this curriculum was designed for senior citizens in the United States.
- While you are welcome to expand on the information provided, note that this guide does not provide detailed instructions on how to change account settings, configure computer settings, or fix technical issues.

Workshop Outline

The below schedule is merely a recommendation. Ultimately, the schedule of your workshop is determined by you (e.g., one-day workshop, one topic per day, one topic per week, etc.)

#	Topic	Duration	Learning Objectives	Additional Resources
1.	Welcome	10 min.	Class and facilitator introductions. Basic program overview. Pre-workshop knowledge survey	CyberGenerations Knowledge Survey Appendix B2
2.	Introduction to Cybersecurity	30 min.	Develop understanding of cybersecurity, include: • Physical threats • Cyber hygiene • Personally identifiable information	
3.	Password Management	30 min.	Understand the importance of creating strong passwords	
4.	Common Internet Threats	45 min.	Identify signs of malware and understand how it spreads	CyberGenerations_ Activities.ppt Appendix A1 Appendix A2 Appendix A5
5.	Internet Scams and Fraud	45 min.	Awareness of common scams. Scam identification. Scam avoidance and remediation.	CyberGenerations_ Activities.ppt Appendix A3 Appendix A4
6.	Social Media Safety and Awareness	45 min.	Identification of social media platforms and their uses. Awareness of social media scams.	
7.	Review Activity: Jeopardy	30 min.	Correctly answer questions on topics covered throughout the workshop	CyberGenerations_ Jeopardy.ppt
8.	Post-Workshop Survey	5 min.	Report attendees' change in knowledge of cybersecurity	CyberGenerations Knowledge Survey Appendix B2
9.	Facilitator Feedback		For Facilitator ONLY	Appendix B1
	Total Duration	**4 hrs.**		

Preparation Notes for Facilitators

Advance Preparation for Facilitators

- **It is highly recommended that you read through the entirety of this facilitator guide prior to hosting the workshop to familiarize yourself with the workshop content and resources.**
  - This Facilitator Guide follows an ASK/SAY/DO format
    - ASK = Ask a question to the audience
    - SAY = Recommended script
    - DO = Action to be taken (open video, etc.)
  - Throughout the guide you will see facilitator notes and the term '*Build.'* A build is a slide animation (appearance of graphic or text). For example, '*This slide has 5 builds'* means you will click/advance the presentation a total of five times while covering the material on that slide. The builds are mentioned in-line with the script.

- **Your introduction to the participants:**
  - An engaging introduction by the Facilitator is an important early step in helping participants feel at ease in the CyberGenerations workshop, informing them of your background and experience, and helping them see how the skills they will learn can be applied in their daily lives. You are encouraged to give careful thought to how you will introduce yourself. Your introduction may include:
    - A brief background of your cybersecurity knowledge.
    - Why you are excited to be facilitating the CyberGenerations workshop.
    - How applicable you feel the content will be to them immediately.
    - The opportunities throughout the CyberGenerations workshop to discuss important concepts and learn from each other.
- Information regarding the logistics that are specific to the venue/location you are delivering the training in, including restroom location, break times, and safety items (fire alarms, evacuation, and so on).

- **Completion of CyberGenerations Knowledge Survey by participants.**
  - Workshop attendees should complete both pre- and post-workshop surveys measuring their perceived knowledge of basic cybersecurity topics. Because the feedback from this survey will be used to make future improvements to the program, completion by attendees is strongly encouraged.
  - The pre-workshop survey is built into the Welcome section of the Facilitator Instructions, and the post-workshop survey is available after the Jeopardy Review. Consider providing a few laptops that the attendees can use to complete the surveys.
  - Attendees with smartphones may complete the surveys on their devices.
  - If you cannot collect responses electronically, a printable copy of the survey is available in Appendix B. We ask that you manually input the feedback into the Google form, or mail the surveys to the CyberPatriot Program Office at 1501 Lee Hwy, Ste 400, Arlington, VA 22209

Facilitator Resources

- **Audio/Visual Requirements**
  - A computer or laptop that can connect to a projector and run Microsoft PowerPoint
  - Internet connection for slides that reference external videos and links.
  - Sound (speakers) for videos.
- **Program Resources**
  - Interest Flyer (editable Word Document)
  - CyberGenerations Workshop Presentation (PowerPoint)
  - CyberGenerations Activities (PowerPoint)
  - CyberGenerations Jeopardy (PowerPoint)
  - Print-out or digital copy (PDF) of this Facilitator Guide
  - Participant Knowledge Survey (Google Form or handout)
  - Facilitator Feedback Survey (Google Form)

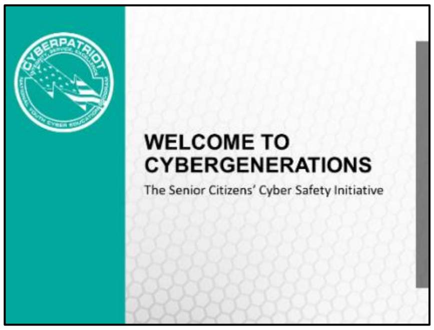
Participant Resources

The following materials are to be available electronically or in print:

- CyberGenerations Knowledge Survey (Google form link or print out in Appendix B)
- CyberGenerations Self-Paced Guide (optional)
  - If providing attendees with self-paced guide, distribute before the workshop begins.
  - The Self-Paced Guide is NOT supposed to act as classroom material. The guide is meant to be a reference point for additional information on the topics discussed during the workshop.

Facilitation Instructions

Topic 1: Welcome (10 min.)



WELCOME TO CYBERGENERATIONS

The Senior Citizens' Cyber Safety Initiative

SAY

Welcome to your CyberGenerations workshop.

DO

Introduce yourself to the participants and allow your Co-Facilitator(s) to do the same (if applicable).

Your introduction may include:

- A brief background of your education or career.
- Why you are excited to be facilitating the CyberGenerations Workshop.
- How you feel the content will be applicable to them immediately.
- Opportunities throughout the workshop to discuss important concepts and learn from each other.

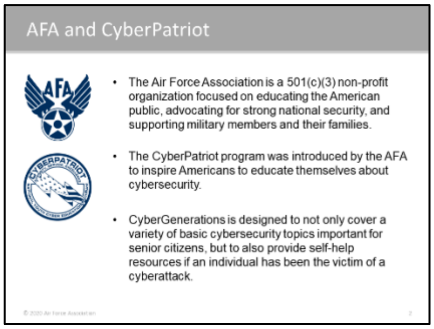
If time allows, participants should introduce themselves to the class, sharing one thing they want to get out of this workshop.

Remind participants about their Self-Paced Guides (if applicable). They can use their self-paced guides to take notes or reference information after the workshop has ended.

DO

Highlight the logistics for the workshop as applicable to your location:

- Start, end and break times, restroom location, evacuation/exit plan in case of emergency, etc.



AFA and CyberPatriot

- The Air Force Association is a 501(c)(3) non-profit organization focused on educating the American public, advocating for strong national security, and supporting military members and their families.
- The CyberPatriot program was introduced by the AFA to inspire Americans to educate themselves about cybersecurity.
- CyberGenerations is designed to not only cover a variety of basic cybersecurity topics important for senior citizens, but to also provide self-help resources if an individual has been the victim of a cyberattack.

© 2020 Air Force Association 2

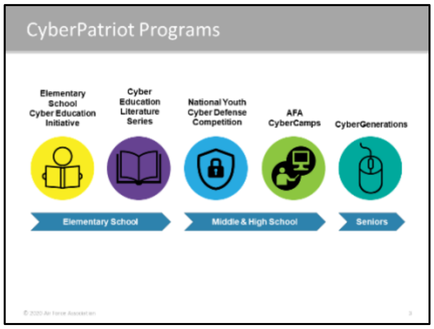
SAY

Let’s start off by discussing the Air Force Association and its CyberPatriot program.

The Air Force Association is a 501(c)(3) non-profit organization dedicated to educating Americans, advocating for aerospace power and STEM education, and supporting military families.

In 2009, the CyberPatriot program was introduced by the Air Force Association to excite and teach our youth about cybersecurity. In 2018, CyberPatriot saw the need to educate older individuals about cybersecurity as well… that's when CyberGenerations was created.

CyberGenerations is designed to not only cover a variety of basic cybersecurity topics important for protecting senior citizens against random cyberattacks, but to also provide supplementary materials and important self-help resources (included in the CyberGenerations Self-Paced Guide).



CyberPatriot Programs

Elementary School Cyber Education Initiative

Cyber Education Literature Series

National Youth Cyber Defense Competition

AFA CyberCamps

CyberGenerations

Elementary School

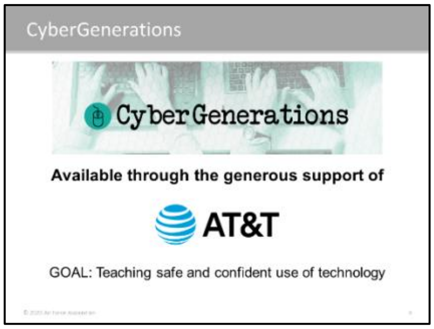
Middle & High School

Seniors

SAY

Before we get into CyberGenerations, let's quickly go over the various programs offered by CyberPatriot (great for grandkids!)

- At the elementary school level CyberPatriot offers a free Elementary School Cyber Education Initiative (ESCEI), and also has two children's books available for purchase through a literature series.
- At the middle school and high school levels, CyberPatriot offers a National Youth Cyber Defense Competition where students learn how to secure computers in a virtual environment. There are also CyberCamps available for novice and advanced students that want to learn more about cybersecurity during the summer months.



CyberGenerations

CyberGenerations

Available through the generous support of

AT&T

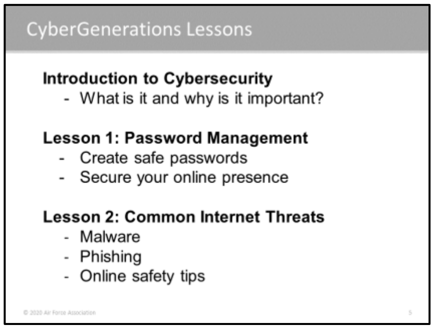
GOAL: Teaching safe and confident use of technology

SAY

AT&T and CyberPatriot collaborated on this program with the goal of teaching safe and confident use of technology to senior citizens. It is designed to encourage you to make wise choices regarding your online and mobile activity.

Thank you for being part of the CyberGenerations initiative and thank you for your commitment to learning more about being safe online.

Facilitator note: The CyberGenerations Self-Paced Guide has additional information for attendees to explore after they have attended this course/workshop. If they have the guide in front of them, encourage them to add additional notes as they go through the workshop.



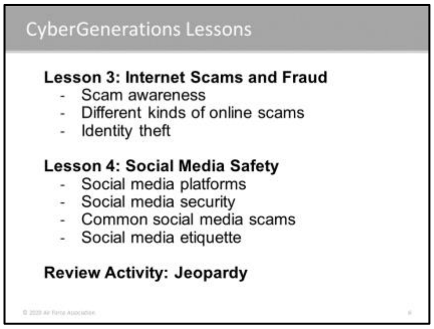
CyberGenerations Lessons

Introduction to Cybersecurity
- What is it and why is it important?

Lesson 1: Password Management
- Create safe passwords
- Secure your online presence

Lesson 2: Common Internet Threats
- Malware
- Phishing
- Online safety tips

© 2020 Air Force Association 5



CyberGenerations Lessons

Lesson 3: Internet Scams and Fraud
- Scam awareness
- Different kinds of online scams
- Identity theft

Lesson 4: Social Media Safety
- Social media platforms
- Social media security
- Common social media scams
- Social media etiquette

Review Activity: Jeopardy

© 2020 Air Force Association 6

DO

Read aloud each lesson that CyberGenerations will cover.

SAY

By the end of this workshop you will have the knowledge and confidence to secure the technology you use every day.

Pre-Workshop Knowledge Survey

http://bit.ly/2Sk9Z5S

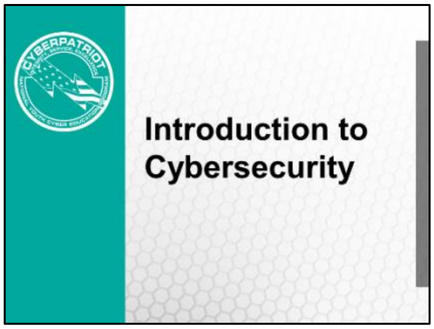
© 2020 Air Force Association 7

SAY

So that we can gauge the effectiveness of this workshop, let’s each take 2-3 minutes to complete the CyberGenerations Knowledge Survey. The same survey will be given at the end of the workshop.

Facilitator Note: Consider providing a few laptops for attendees to use to complete the survey. Attendees with smartphones may complete the survey on their devices by scanning the QR code with their phone cameras or visiting the URL.

Topic 2: Introduction to Cybersecurity (30 min.)

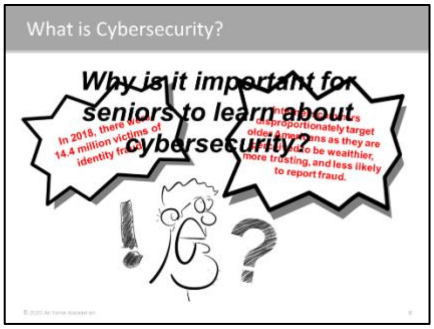


Introduction to Cybersecurity

SAY

Before anything else, we need to understand what cybersecurity means, and why it's so important to have good cybersecurity practices.

Cybersecurity



What is Cybersecurity?

Why is it important for seniors to learn about cybersecurity?

In 2018, there were 14.4 million victims of identity fraud.

Internet scammers disproportionately target older Americans as they are perceived to be wealthier, more trusting, and less likely to report fraud.

This slide has 1 build.

ASK

Why is it important for seniors to learn about cybersecurity?

SAY

Online fraud is the most common crime in the US. Almost one in ten people fall victim to identity fraud.

Build 1

In 2018, there were 14.4 million victims of identity fraud.

According to the FBI, internet scammers disproportionately target older Americans as they are wealthier, more trusting, and less likely to report fraud.

Knowing this, it's particularly important for the senior citizens to familiarize themselves with the different scams and dangers on the internet and learn about how they can protect themselves in order to have a safe and positive experience online.

What is Cybersecurity?

Cybersecurity is the protection of internet-connected systems – including hardware, software, and data – from cyberattacks.

AT&T
Quiz: How Cybersecure are You?
How do you score when it comes to protecting your accounts, devices and information? Take our Cyber Aware quiz to see.
Take the Quiz

This slide has 1 build.

This slide links to an external resource.

ASK

You've heard the term cybersecurity, but can anybody define it?

Expected responses include:

- Staying safe online
- Protecting information on computer

Build 1

SAY

Cybersecurity is the protection of internet-connected systems – including hardware, software, and data – from cyberattacks.

It is important to be aware of cyber threats because they affect all of us. Cybercrime is one of the toughest challenges that the world is facing today, and it's set to cost organizations and individuals up to $6 trillion annually by 2021.

Before we get into the details of cybersecurity, let's see how cyber-secure this class is in their daily lives.

DO

Open the *AT&T Cyber Aware quiz – How Cybersecure Are You? Assess Your Personal Risk* (click the image)

Facilitator Note: Complete the quiz as a group. Participants may raise their hands to answer Yes or No. Choose the majority answer and move forward to the next question.

What is Cybersecurity?

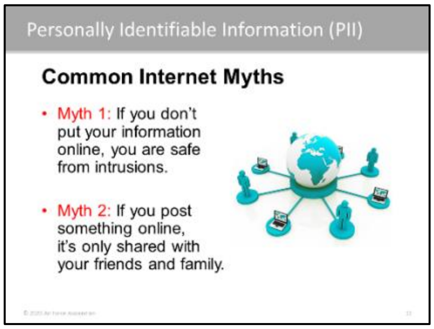
Video: Explanation of Cybersecurity

This slide links to an external resource.

DO

Open the *Cybersecurity Explained* video (click the image)

Personally Identifiable Information



Personally Identifiable Information (PII)

Common Internet Myths

- Myth 1: If you don't put your information online, you are safe from intrusions.
- Myth 2: If you post something online, it's only shared with your friends and family.

ASK

Why is it important to be safe online?

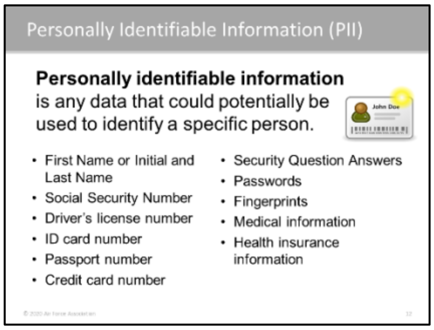
Expected responses include:

- Protect your information
- Avoid scams or fraud

SAY

Lots of our data is stored online or on computers. Even if you don't use computers regularly, it is still possible that your information is at risk. Two myths associated with using the internet are:

- Myth 1: If you don't put your information online, you are untraceable and therefore safe from intrusions.
  - Truth: Publicly available government records, court records, or records of any organization or committee that you are a member of are all viable sources of personal information.
- Myth 2: If you post something online, it's only shared with your family and friends.
  - Truth: The internet is a mysterious place and you never know where your information will end up. Even if you are being careful and deleting data which exposes personal information, there's always a chance that your information has been copied and stored somewhere else and can be accessed by criminals.



Personally Identifiable Information (PII)

Personally identifiable information is any data that could potentially be used to identify a specific person.

- First Name or Initial and Last Name
- Social Security Number
- Driver's license number
- ID card number
- Passport number
- Credit card number
- Security Question Answers
- Passwords
- Fingerprints
- Medical information
- Health insurance information

This slide has 1 build.

SAY

One of the biggest goals of cybersecurity is protecting personally identifiable information (PII). Personally identifiable information is any data that could potentially be used to identify a specific person.

ASK

Who can tell me some examples of PII?

> *Facilitator Note: Allow participants to yell out answers*

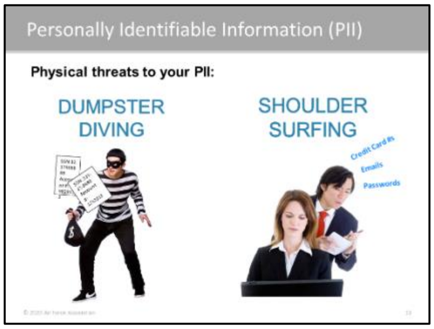
Build 1

DO

Read through the examples of personally identifiable information.

SAY

Any of this information getting into the hands of an untrustworthy source could lead to fraud or identity theft. It's important to treat your PII like you would a precious valuable!



Personally Identifiable Information (PII)

Physical threats to your PII:

DUMPSTER DIVING

SHOULDER SURFING

This slide has 2 builds.

SAY

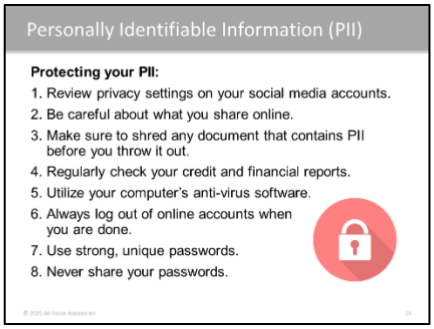
Sharing this information isn't the only way for people to gain access to it. There are also physical threats to how PII can be obtained.

Build 1

Dumpster diving… this actually happens. Thieves will sift through garbage for receipts with credit card information, medical forms with social security numbers, or other documents with personal information. They can use that information to impersonate you for financial gains or to access confidential information.

Build 2

Another way people steal your information is through shoulder surfing. People can learn a lot about your personal information by simply looking over your shoulder while you type. Be careful when typing personal information including passwords. In public areas, lower your screen so only you can see it.



Personally Identifiable Information (PII)

Protecting your PII:

1. Review privacy settings on your social media accounts.
2. Be careful about what you share online.
3. Make sure to shred any document that contains PII before you throw it out.
4. Regularly check your credit and financial reports.
5. Utilize your computer's anti-virus software.
6. Always log out of online accounts when you are done.
7. Use strong, unique passwords.
8. Never share your passwords.

© 2020 Air Force Association 14

SAY

The steps you can take to protect your PII are all steps that will be covered in this workshop.

- Review privacy settings on your social media accounts – Try to keep up with the changing privacy and security settings on different websites and make sure that all of your online accounts are safe and secure.
- Be careful about what you share online – Avoid sharing personal information that might give away vital details about you to would-be criminals.
- Make sure to shred any document that contains PII before you throw it out to keep personal information out of the hands of the wrong people
- Regularly check your credit and financial reports – This will help you avoid credit fraud and lessen the possibilities of identity theft.
- Utilize your computer's anti-virus software – Anti-virus/anti-malware software are often pre-installed on your computer and they are essential for securing your device.
- Always log out of online accounts when you are done – This is especially important if you are using a computer in a public place.
- Use strong, unique passwords – In the next lesson, we will discuss the advantages of having a strong password.
- Never share your passwords – Be wary about sharing your passwords and avoid writing them down anywhere.

Mobile Devices

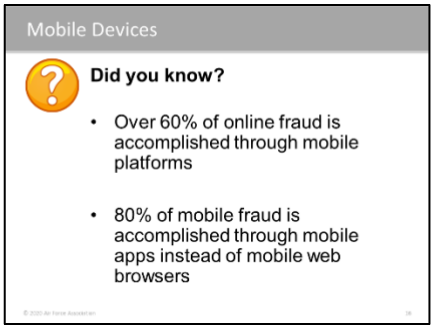
Mobile Devices

Mobile devices are portable or handheld devices that have data or can connect to another device that has data.

© 2020 Air Force Association 15

SAY

Mobile devices are portable or handheld devices that have data or can connect to another device that has data. Just like computers, mobile devices are susceptible to cyberattacks and need to be protected.



Mobile Devices

Did you know?

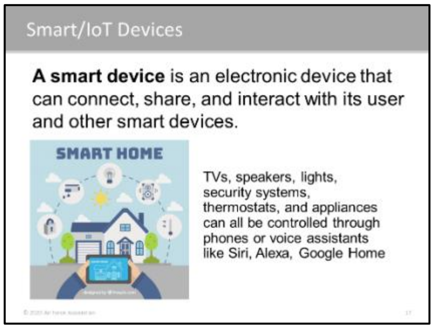
- Over 60% of online fraud is accomplished through mobile platforms
- 80% of mobile fraud is accomplished through mobile apps instead of mobile web browsers

© 2020 Air Force Association 16

SAY

According to the 2018 Current State of Cybercrime White Paper by RSA, a cybersecurity and digital risk management solutions company, over 60% of online fraud is accomplished through mobile platforms.

Additionally, 80% of mobile fraud is accomplished through mobile apps instead of mobile web browsers.



Smart/IoT Devices

A smart device is an electronic device that can connect, share, and interact with its user and other smart devices.

TVs, speakers, lights, security systems, thermostats, and appliances can all be controlled through phones or voice assistants like Siri, Alexa, Google Home

© 2020 Air Force Association 17

SAY

One step beyond mobile devices are Smart/Internet of Things (IoT) Devices. IoT devices are creating “smart homes” everywhere. Consumer connected devices include TVs, speakers, lights, security systems, thermostats, and appliances that can all be controlled through phones or voice-activated assistants like Siri, Alexa, or Google Home.

Smart/IoT Devices

Cyber Aware Smart Risk Tip:

It's very important to know how you can secure smart devices. Some important tips are:

- Stay up to date on software updates.
- Change default passwords.
- Disconnect when not in use.
- Be careful about the smart device apps you install and use.

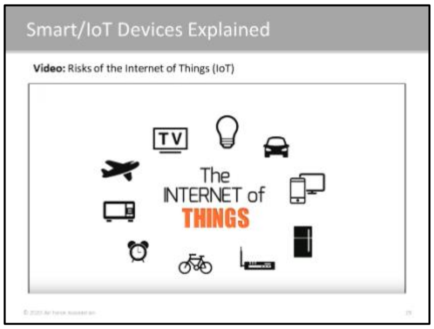
© 2020 Air Force Association 18

SAY

It’s especially important to know how to protect these smart devices from attack. AT&T recommends these steps to secure such devices:

- Stay up to date on software updates.

- Change default passwords.
- Disconnect when not in use (not applicable to voice-activated devices).
- Be careful about the smart device apps you install and use.



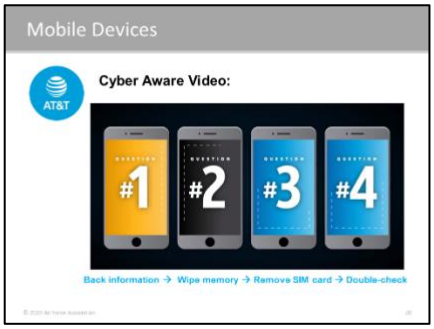
Smart/IoT Devices Explained

Video: Risks of the Internet of Things (IoT)

This slide links to an external resource.

DO

Open the *Risks of the Internet of Things* video (click the image)



Mobile Devices

Cyber Aware Video:

Back information → Wipe memory → Remove SIM card → Double-check

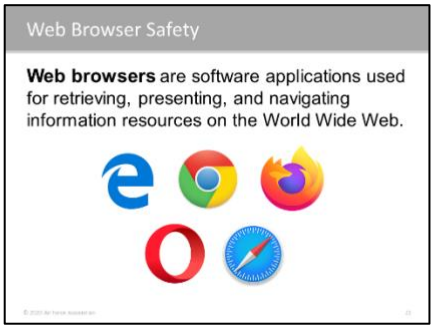
SAY

Should you need to get a new phone, it’s important that you clear the data from your old phone before turning it in. The last thing you want to do is give away your personal information when you give away your phone. This helpful video from AT&T shows the steps you should take to secure your device before turning it in.

DO

Open the *Device Trade In* video (click the image)

Web Browser Safety



Web Browser Safety

Web browsers are software applications used for retrieving, presenting, and navigating information resources on the World Wide Web.

This slide has 1 build.

SAY

A lot of time when we use the internet, we are using a web browser.

- A web browser is a software application used for retrieving, presenting, and navigating information resources on the World Wide Web.
- When we want to ‘google’ something, or sign into our bank account, we must use a web browser to do so.

ASK

Can anybody give me an example of a web browser?

Expected responses include:

- Explorer/Edge
- Google Chrome
- Mozilla Firefox

Build 1

SAY

Internet Explorer, Google Chrome, Mozilla Firefox, Opera, and Safari are common web browsers

Web Browsing Safety

Video: How to Know if a Website is Secure

This slide links to an external resource.

SAY

With the number of hackers and scammers out there, it can be tough to know if a website is safe. Fortunately, there are safety features in place to help you know. This video will explain those features.

DO

Open the *How to Know if a Website is Secure* video (click the image)

Topic 3: Password Management (30 min.)

Password Management

ASK

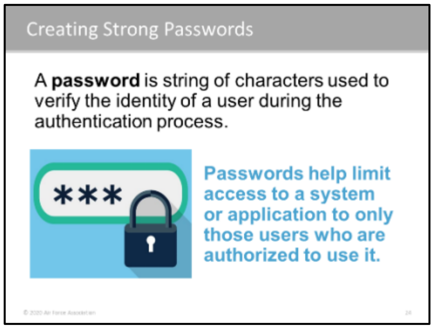
How do you use passwords in your daily life?

Do you remember the first time you used a password? What was the password for?

SAY

Hopefully you are all familiar with passwords. In this section we'll cover why creating strong passwords is important and the steps you can take to manage passwords for your accounts.

Creating Strong Passwords



Creating Strong Passwords

A **password** is string of characters used to verify the identity of a user during the authentication process.

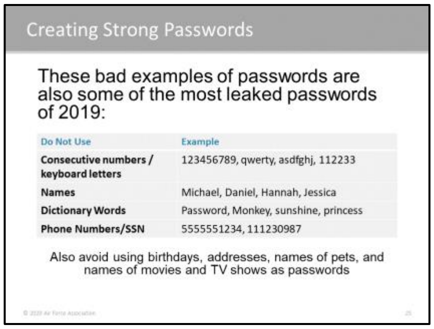
Passwords help limit access to a system or application to only those users who are authorized to use it.

© 2020 Air Force Association 24

SAY

Passwords help protect our personal information on the internet, and they are often the only things standing between cyber criminals and our sensitive data.

- A strong password is not only important, but absolutely necessary.



Creating Strong Passwords

These bad examples of passwords are also some of the most leaked passwords of 2019:

Do Not Use	Example
Consecutive numbers / keyboard letters	123456789, qwerty, asdfghj, 112233
Names	Michael, Daniel, Hannah, Jessica
Dictionary Words	Password, Monkey, sunshine, princess
Phone Numbers/SSN	5555551234, 111230987

Also avoid using birthdays, addresses, names of pets, and names of movies and TV shows as passwords

SAY

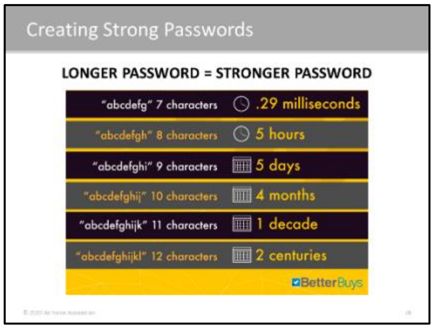
These are some of the worst passwords you could use. Most of them made the list of top 100 leaked passwords in 2019.

DO

Review each example from the table on the slide.

SAY

You also want to avoid passwords that people could guess based on things they know about you, like your birthday, address, name of your pet, or the name of your favorite movie.



Creating Strong Passwords

LONGER PASSWORD = STRONGER PASSWORD

"abcdefg" 7 characters	.29 milliseconds
"abcdefgh" 8 characters	5 hours
"abcdefghi" 9 characters	5 days
"abcdefghij" 10 characters	4 months
"abcdefghijk" 11 characters	1 decade
"abcdefghijkl" 12 characters	2 centuries

BetterBuys

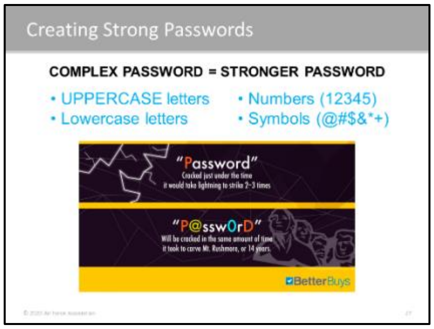
SAY

Hackers use algorithms and sophisticated programs to crack passwords. So, the longer the password is, the more difficult it is to crack.

Adding a single character to a password boosts its security exponentially.

DO

Refer to graphic on slide. Review times it takes to crack each password.



Creating Strong Passwords

COMPLEX PASSWORD = STRONGER PASSWORD

- UPPERCASE letters
- Lowercase letters
- Numbers (12345)
- Symbols (@#$&*+)

"Password"
Cracked just under the time
it would take lightning to strike 2-3 times

"P@ssw0rD"
Will be cracked in the same amount of time
it took to carve Mt. Rushmore, or 14 years.

BetterBuys

17

This slide links to an external resource.

SAY

Complex passwords can also contribute towards additional protection. To make a password harder to crack, always use a combination of:

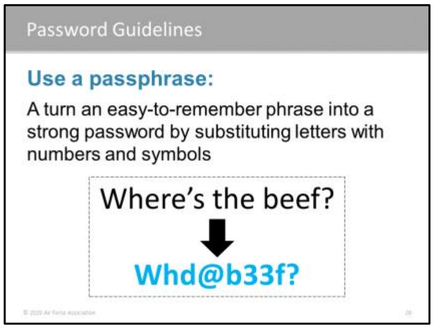
- UPPERcase letters
- Lowercase letters
- Numbers
- Symbols

A simple, common word can be cracked in fractions of a millisecond. Mix in lowercase and uppercase letters, numbers, and symbols (think @, %, and #), and your password can be secure for more than a decade.

DO

Click the graphic to open Better Buys Password-Cracking Times. Type in examples of good and bad passwords to show audience the difference in the amount of time it takes to crack weak passwords versus strong passwords.

Password Guidelines



Password Guidelines

Use a passphrase:

A turn an easy-to-remember phrase into a strong password by substituting letters with numbers and symbols

Where's the beef?

⬇

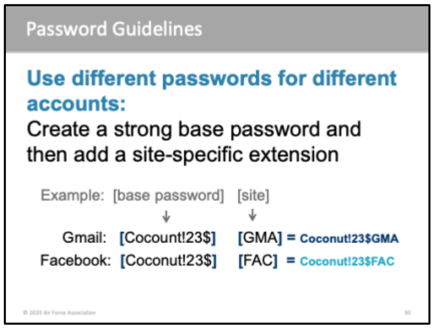
Whd@b33f?

18

SAY

Another way to increase password strength is to use a 'Passphrase':

- A passphrase is a short phrase used as a password in which you can substitute letters with symbols and numbers.
- Make sure that it's a random sentence that has some meaning to you and not a famous quote or phrase.



Password Guidelines

Use different passwords for different accounts:

Create a strong base password and then add a site-specific extension

Example:	[base password]	[site]	
	↓	↓	
Gmail:	[Cocount!23$]	[GMA]	= Coconut!23$GMA
Facebook:	[Coconut!23$]	[FAC]	= Coconut!23$FAC

30

This slide has 1 build.

SAY

73% of people use the same passwords for all or most of their accounts.

ASK

Why is it a bad idea to use the same password for your Facebook, email, banking, or healthcare accounts?

SAY

If you use the same password for every account, a breach in one system could make your other accounts vulnerable as well.

Having multiple passwords can be hard to remember. A simple trick is to start with a base password and then add an abbreviation to the beginning or end that reminds you what account it is for.

Build 1

Starting with a base password, we can add GMA to signify Gmail and FAC to signify Facebook. You could add any prefix or suffix you would like, as long as you remember what it stands for.

Password Guidelines

Change passwords often:

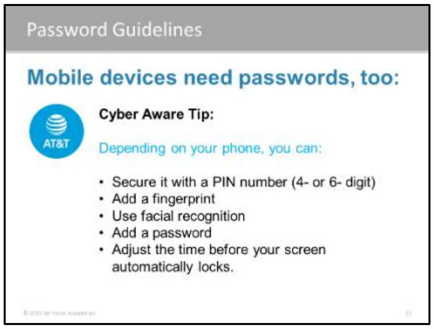
Change your password every 6-12 months

SAY

The longer you keep a password, the longer attackers can attempt to crack it.

If your password is vulnerable and is at risk of falling into the wrong hands, then changing your password often will shorten the amount of time a criminal might have to access your information using the weak password.

- The recommended time for changing passwords is once every 90 days. But if this is too often for you, make sure to change your passwords at least once every 6-12 months.



Password Guidelines

Mobile devices need passwords, too:

Cyber Aware Tip:

Depending on your phone, you can:

- Secure it with a PIN number (4- or 6- digit)
- Add a fingerprint
- Use facial recognition
- Add a password
- Adjust the time before your screen automatically locks.

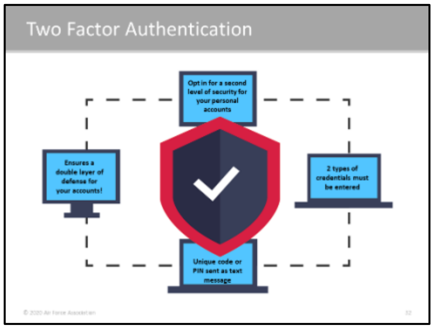
ASK

By a show of hands, how many of you have a password to unlock your phones or tablets?

SAY

Mobile devices need passwords, too, because mobile devices store personal information. According to AT&T, it is recommended you do the following, depending on your phone type:

- Secure it with a PIN number (4- or 6- digit)
- Add a fingerprint
- Use facial recognition
- Add a password
- Adjust the time before your screen automatically locks.



Two Factor Authentication

Opt in for a second level of security for your personal accounts

Ensures a double layer of defense for your accounts!

2 types of credentials must be entered

Unique code or PIN sent as text message

32

SAY

Many websites today use two-factor authentication when a person is trying to sign-in. Two-factor authentication is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access.

For example, after inputting your password, the site may also send a text to your phone with a code or PIN that must be entered to gain access to your account. Generally, you need two of these three pieces of information:

- Something you know, such as a personal identification number (PIN), password or a pattern.
- Something you have, such as an ATM card, phone, or fob.
- Something you are, such as a biometric (fingerprint or voice print).

A simple search on the internet can tell you exactly how to turn on two-factor identification for different websites.

Password Management Systems

Password Management System

Password management systems store your login information for all the websites you use and help you log into them automatically

Recommended systems:

LastPass

dashlane

1Password

© 2020 Air Force Association 33

SAY

A password management system is a software application that stores and manages a user's passwords for various online accounts. A user can store account log-in information for all their accounts in one place, therefore only having to remember one main password.

ASK

Does anybody here already use a password management system?

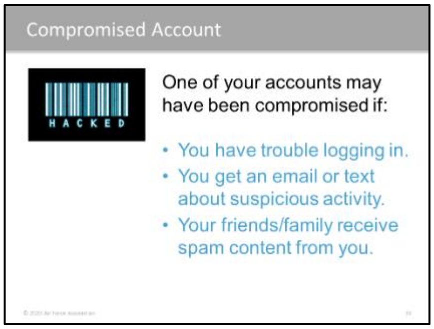
> *Facilitator note: If yes, ask which systems? If no, mention recommended systems shown on the slide.*

SAY

One thing to keep in mind, however, is that you shouldn't rely on password management systems that are built into web browsers.

- Browsers like Google Chrome will ask if you want to save a password or "auto-fill" information. You should always click No. They can't compete with dedicated services which have a lot of useful features, offer a more powerful interface, and are a lot more secure.

Compromised Account



Compromised Account

One of your accounts may have been compromised if:

- You have trouble logging in.
- You get an email or text about suspicious activity.
- Your friends/family receive spam content from you.

© 2020 Air Force Association [illegible]

This slide has 3 builds.

ASK

How do you think you can tell if one of your accounts has been compromised?

> *Answer expectations:*

- Cannot log in
- Alert from company
- Unusual activity / spending

SAY

Build 1

If you have trouble logging in – then you should know that someone might have accessed your account and changed the password.

Build 2

Online applications can often send you notifications about suspicious activities – like your account being accessed from a new device or from a strange location. Always verify such activities and change your password immediately.

Build 3

Sometimes your friends might alert you about spam content being sent using your account. This is a red flag and you should take the necessary steps to secure your account again.

Always change your password whenever an account is compromised.

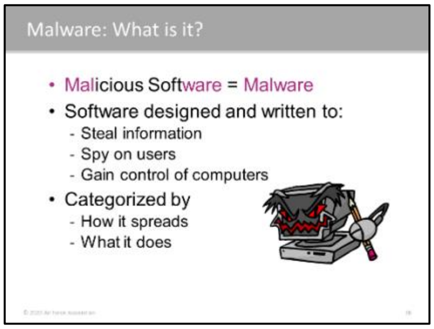
Topic 4: Common Internet Threats (45 min.)

Common Internet Threats

SAY

In this section you will learn about the various threats seen on the internet, including malware, spoof emails/calls/texts and the different kinds of social engineering. More importantly, you will learn easy-to-remember tips on how to avoid these common threats.

Malware



Malware: What is it?

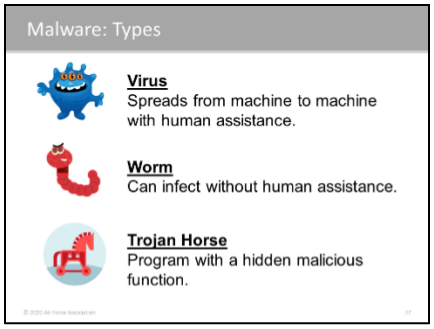
- Malicious Software = Malware
- Software designed and written to:
  - Steal information
  - Spy on users
  - Gain control of computers
- Categorized by
  - How it spreads
  - What it does

© 2020 Air Force Association 16

SAY

Malware (malicious software) is a term for any software that is intentionally designed to cause harm or do illegal and unethical things.

- Malware can be used to steal information, spy on people or organizations, gain control over computer systems, or launch huge cyberattacks.
- Malware is classified by how it spreads from computer to computer and what it does when it has infiltrated a system.



Malware: Types

Virus
Spreads from machine to machine with human assistance.

Worm
Can infect without human assistance.

Trojan Horse
Program with a hidden malicious function.

© 2020 Air Force Association 37

SAY

Now let’s look at specific examples of malware:

- The most commonly known type of malware is a virus. Viruses spread from machine to machine with the aid of unwitting humans.

ASK

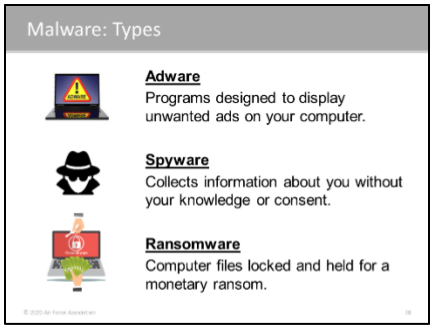
Any idea how your device can get infected with a virus?

Answer expectations:

- *Email attachments*
- *Malicious websites*
- *Spoofed links*
- *Downloaded or shared files like “free” movies*

SAY

- Next, we have worms. Worms don’t need the assistance of humans to spread. They scan networks until they find weaknesses and then attack.
- Trojan Horses are also sometimes referred to as trojan viruses or just trojans. Computers are infected when a user downloads or access files that he or she believes are valid and safe. These might be email attachments, shared files like Torrent files, or media, software, or document files downloaded online.



Malware: Types

Adware
Programs designed to display unwanted ads on your computer.

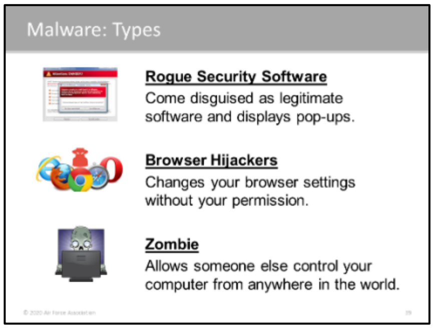
Spyware
Collects information about you without your knowledge or consent.

Ransomware
Computer files locked and held for a monetary ransom.

© 2020 Air Force Association 38

SAY

- Adware displays unwanted ads on your computer. It redirects you to advertising websites and might be secretly collecting data about your online activities.
- Spyware programs automatically take regular screenshots of an infected system and transmit them to the attacker. Others are used by attackers to launch spam ads through the Internet. These spyware programs are often plugins that log and transmit your Internet activity and use it to create targeted pop-ups and advertisements.
- Ransomware is the kidnapping of your computer data. It’s a type of malware in which the attacker encrypts the victim’s data and demands payment for the encryption key. Ransomware spreads through email, attachments, infected programs, and compromised websites.
    - According to AT&T, ransom demands for account and devices are on the rise, and bad guys are requesting payment in cryptocurrency (bitcoin, etc.) because it is not traceable or insured, so you cannot recover it when it’s gone.
    - If you think you are the victim of ransomware, change your password immediately, do not reply or click on any links, and most importantly, DO NOT SEND MONEY.



Malware: Types

Rogue Security Software
Come disguised as legitimate software and displays pop-ups.

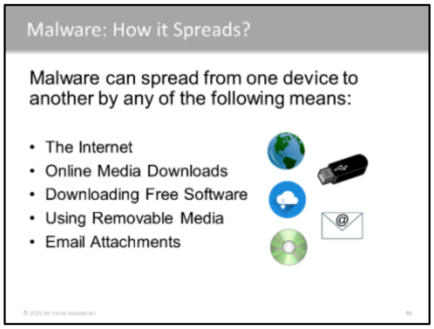
Browser Hijackers
Changes your browser settings without your permission.

Zombie
Allows someone else control your computer from anywhere in the world.

© 2020 Air Force Association 39

SAY

- Rogue Security Software usually comes disguised as legitimate software like anti-virus software. It usually displays bothersome pop-up messages persistently and might prompt the victim to pay money to fix the made-up problems.
- A Browser Hijacker can change your browser settings without your permission, inject unwanted ads into your web browser, or replace your home page with the hijacker page. It might also contain spyware to steal sensitive information from your device.
- Zombie software makes it possible for someone else to control your computer from anywhere in the world. Once a computer has been infected, it is referred to as a “zombie” or as a “bot”, which is short for robot. Bad guys who distribute zombie software try to install it on as many computers as possible.



Malware: How it Spreads?

Malware can spread from one device to another by any of the following means:

- The Internet
- Online Media Downloads
- Downloading Free Software
- Using Removable Media
- Email Attachments

This slide has 5 builds

ASK

It was mentioned earlier, but how do you think malware spreads?

SAY

Build 1

- The Internet: Visiting infected websites can expose your device to many types of malware. Once your device is infected, it becomes a repository and can infect other computers easily.

Build 2

- Online Media Downloads: Downloading movies, TV shows, or music from questionable online sources for free is not only illegal but can be potentially dangerous for your device.

Build 3

- Downloading Free Software: If you are downloading software for free (Freeware and Shareware), there’s a good chance that you are also downloading undesirable programs along with the software.

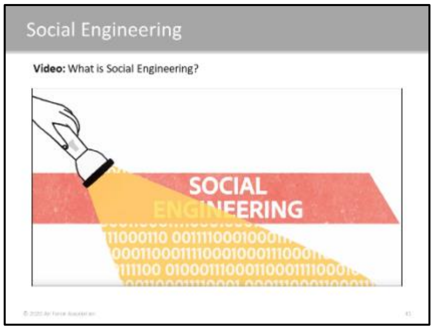
Build 4

- Using Removable Media: Malware can spread from one computer to the other very easily through removable media like DVDs or USB thumb drives.

Build 5

- Email Attachments: If you receive unsolicited emails with suspicious attachments, you should never download them. The attachments are often malware.

Social Engineering



Social Engineering

Video: What is Social Engineering?

This slide links to an external resource.

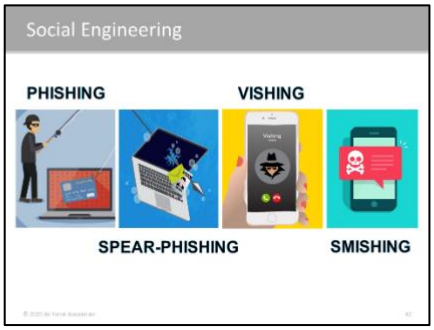
SAY

Manipulating people into giving up personal information is called Social Engineering. For example, pretending to be your friend online, or giving a false reason for needing some personal information would be Social Engineering.

This 2-minute video does a great job explaining what social engineering looks like.

DO

Open the *What is Social Engineering?* video (click the image)



Social Engineering

PHISHING

VISHING

SPEAR-PHISHING

SMISHING

This slide has 4 builds

SAY

These are some of the main methods that social engineers use to extract information from you.

Build 1

- Phishing refers to spoofing or fraud attempts perpetrated by random attackers against a wide number of users, for example fraudulent emails and websites.

Build 2

- Social engineers can go one step further and send a spoof from an organization with whom the user is known to be associated, or even a spoof tailored specifically for the user. This type of phishing is called spear-phishing.

Build 3

ASK

Vishing – Can anyone guess what vishing is?

SAY

Vishing refers to attempts by thieves to obtain confidential information over the phone.

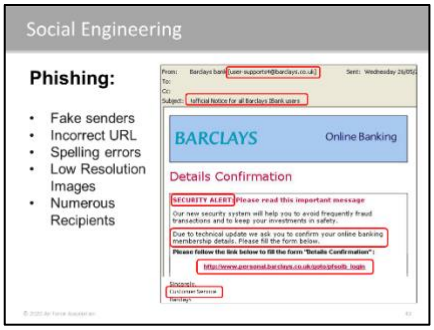
Build 4

ASK

What about smishing?

SAY

Smishing refers to phishing attempts sent by text messages (SMS messages).



Social Engineering

Phishing:

- Fake senders
- Incorrect URL
- Spelling errors
- Low Resolution Images
- Numerous Recipients

From: Barclays bank [user-supports4@barclays.co.uk] Sent: Wednesday 26/05/
To:
Cc:
Subject: !official Notice for all Barclays IBank users

BARCLAYS Online Banking

Details Confirmation

SECURITY ALERT: Please read this important message

Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety.

Due to technical update we ask you to confirm your online banking membership details. Please fill the form below.

Please follow the link below to fill the form "Details Confirmation":

http://www.personal.barclays.co.uk/goto/pfsolb_login

Sincerely,
Customer Service
Barclays

SAY

Now let's look more closely at phishing, vishing, and smishing.

ASK

By a show of hands, who here has ever received a suspicious email from a company, but wasn't sure of its authenticity?

SAY

This example of a spam email has clues for what to look for to identify the legitimacy of emails you receive from a company or organization. The user received an email from their financial institution, it looks real but let's take a closer look at some specific details:

- Look at the email address of the sender: user-supports4@Barclays.co.uk (questionable identity: think, why does it say user-supports4?).
- Now the Subject: this subject has an obvious spelling error/typo (an automated email from a company will rarely have a typo).
- The text in an email is the most important. Think to yourself: Are caps appropriate? Why are they asking me for personal information over email?
- Be wary of links or attachments. You can hover your mouse over the link and see its true destination, you can google the site and see if it comes back as a safe site, question if the link looks fishy – if it does, DO NOT CLICK.
- Authentic emails are almost always signed by individuals.

A scam is never totally obvious. It's up to the user to question and think of the reason behind the email received. When in doubt, call the institution directly. It never hurts to go to the direct source.

Social Engineering

Cyber Aware Video:

Vishing: Neighbor Spoofing uses number that look like they are from your area

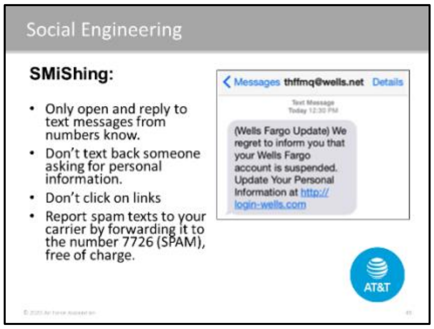
This slide links to an external resource.

SAY

Neighbor spoofing is a particularly devious method used for vishing attempts whereby the criminals try to trick people into answering calls by mimicking their number or by using a number that looks like someone is calling from the same area as them.

DO

Open the *Cyber Aware Neighbor Spoofing* video (click the image).



Social Engineering

SMiShing:

- Only open and reply to text messages from numbers know.
- Don’t text back someone asking for personal information.
- Don’t click on links
- Report spam texts to your carrier by forwarding it to the number 7726 (SPAM), free of charge.

< Messages thffmq@wells.net Details

Text Message
Today 12:30 PM

(Wells Fargo Update) We regret to inform you that your Wells Fargo account is suspended. Update Your Personal Information at http://login-wells.com

SAY

Smishing is a text message that leads you to a fake website that imitates a real company. That site will ask for personal information – username, password or credit card information. It’s called Smishing because texts are actually called "short message system" or SMS.

AT&T recommends the following steps for protecting yourself against smishing:

- Only open and reply to text messages from numbers you know and trust.
- Don’t text back someone who is asking for personal information.
- Don’t click on links included in a text message.
- You can report spam texts to your carrier by forwarding it to the number 7726 (SPAM), free of charge.

Avoiding Common Internet Threats

Avoiding Common Internet Threats

Video: Be Careful with Malware

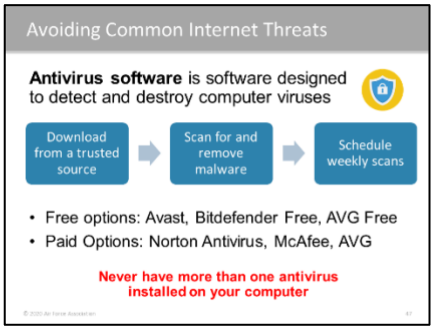
This slide links to an external resource.

SAY

This video was created by Google. It discusses the basics of how to protect computers from malware and how to report threats, so others do not become infected.

DO

Open the *Be Careful with Malware* video (click the image)



Avoiding Common Internet Threats

Antivirus software is software designed to detect and destroy computer viruses

Download from a trusted source → Scan for and remove malware → Schedule weekly scans

- Free options: Avast, Bitdefender Free, AVG Free
- Paid Options: Norton Antivirus, McAfee, AVG

Never have more than one antivirus installed on your computer

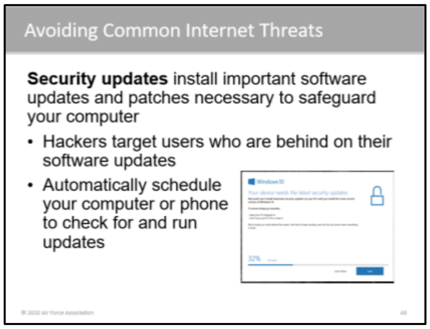
ASK

Does anyone know what antivirus or anti-malware software is or how it works?

SAY

Antivirus software is software designed to detect and destroy computer viruses.

- When you install, make sure you are only installing and running one antimalware/antivirus software on your machine. If you try to run two or more, they may conflict with each other.
- Be very careful when choosing antivirus software. Make sure you are downloading the program you selected from a trusted source and not from a spoofed URL.
- Sometimes computers are sold with antimalware/antivirus pre-installed. If your machine does not have one already installed, take advantage of a trusted free program.
    - Free options include Avast, Bitdefender Free, AVG Free
    - Paid options include Norton Antivirus, McAfee, AVG



Avoiding Common Internet Threats

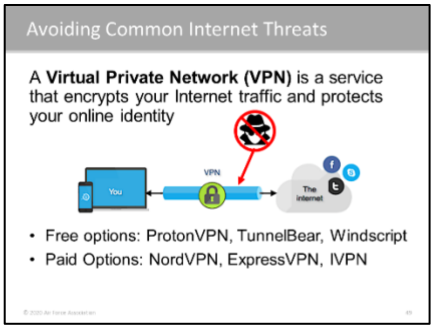
Security updates install important software updates and patches necessary to safeguard your computer

- Hackers target users who are behind on their software updates
- Automatically schedule your computer or phone to check for and run updates

SAY

Security updates are important for keeping your device's security up to date.

- Settings allow for updates to be automatically installed.
- Failure to install updates makes you a target for hackers.



Avoiding Common Internet Threats

A **Virtual Private Network (VPN)** is a service that encrypts your Internet traffic and protects your online identity

You
VPN
The Internet

- Free options: ProtonVPN, TunnelBear, Windscript
- Paid Options: NordVPN, ExpressVPN, IVPN

SAY

Another way to help keep malware from ending up on your computer is by using a virtual private network.

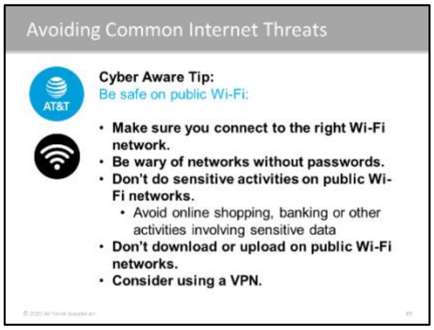
A Virtual Private Network (VPN) is a service that encrypts your internet traffic and protects your online identity.

DO

Refer to graphic on slide.

SAY

- You can subscribe to a legitimate VPN service and pay a monthly fee for the use of the VPN app.
- You can also purchase a VPN connection through your cell phone or internet provider.
- Make sure to do proper research and then choose a VPN service that's reputable and reliable.



Avoiding Common Internet Threats

Cyber Aware Tip:
Be safe on public Wi-Fi:

- **Make sure you connect to the right Wi-Fi network.**
- **Be wary of networks without passwords.**
- **Don't do sensitive activities on public Wi-Fi networks.**
  - Avoid online shopping, banking or other activities involving sensitive data
- **Don't download or upload on public Wi-Fi networks.**
- **Consider using a VPN.**

SAY

Lastly, it's important to choose your internet connection wisely. Sometimes, for example, in airports or shopping malls, we have to use public Wi-Fi connections. If doing so, you should follow these rules to keep your information as secure as possible.

- Make sure you connect to the right Wi-Fi network.
- Be wary of networks without passwords.
- Avoid online shopping, banking or other activities involving sensitive data.
- Do NOT download or upload files on public Wi-Fi networks.
- Consider using a VPN.

Facilitator Note: Optional review activities available. See Appendix A1, A2, and A5.

Topic 5: Internet Scams & Fraud (45 min.)

Internet
Scams & Fraud

ASK

Has anyone in this room been the victim of a fraud or scam?

SAY

It’s estimated that older adults in the United States lose $3.78 billion each year as a result of fraud and financial exploitation.

In this section we will cover the various types of scams on the internet and how to recognize them.

Types of Scams

Types of Scams

Government Agencies
IRS, FBI, FTC, etc.

Financial Institutions
Bank, PayPal, 401K

Insurance Companies
Home, Health, Car

Donation Organizations
Unknown or newly formed

Dating Sites
Fake Sites

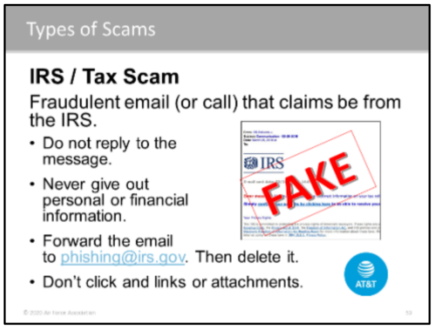
Online/Phone Surveys
Claim to be service providers

DONATE
SURVEY

SAY

Almost any type of organization has its fair share of scammers.

- Common agency scams stem from the IRS, FBI and the Federal Trade Commission. While these scams genuinely do not come directly from the government agencies, this is a typical scam that many people fall victim to.
- Financial and investment companies are easy targets, with so many people signed up for online banking and alerts.
  - Be assured, financial institutions will never ask for personal information through email and will not ask you for personal information during an unsolicited call.
- Dating sites, online and phone surveys as well as false correspondence from donation organizations are just a few more examples of potential scam risks.
  - One of the most important tips to remember is that you are never obligated to share information if you feel uncomfortable.
  - If you question the authenticity of any call or email, it is best to contact the company directly (using the number on their website) to verify the authenticity of the caller.



Types of Scams

IRS / Tax Scam

Fraudulent email (or call) that claims be from the IRS.

- Do not reply to the message.
- Never give out personal or financial information.
- Forward the email to phishing@irs.gov. Then delete it.
- Don't click and links or attachments.

IRS
FAKE
AT&T

SAY

An IRS phishing scam is an unsolicited, fraudulent email that claims to come from the IRS. Some emails link to fake websites which look real. The goal is to lure victims to give up their personal and financial information. If the thieves get what they're after, they use it to steal a victim's money and/or identity.

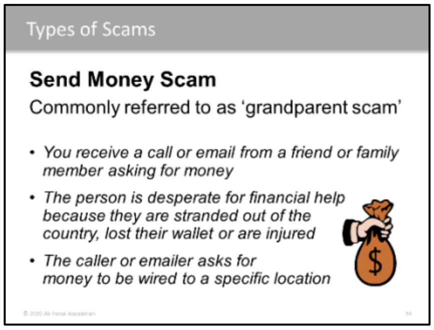
ASK

Have any of you ever received such communication and if so, what did you do?

SAY

If you think you've received an IRS scam phone call or email:

- Hang up or delete the message.
- Never give out personal or financial information.
- Report the email to phishing@irs.gov.



Types of Scams

Send Money Scam

Commonly referred to as 'grandparent scam'

- *You receive a call or email from a friend or family member asking for money*
- *The person is desperate for financial help because they are stranded out of the country, lost their wallet or are injured*
- *The caller or emailer asks for money to be wired to a specific location*

SAY

In a send money scam (also referred to as a grandparent scam), fraudsters either pretend to be the victim's grandchild, friend or some other family member.

- The imposters claim that they are in trouble and need money to help with an emergency (e.g., getting out of jail, paying a hospital bill, or leaving a foreign country).
- These scams tend to target senior citizens. If you receive a phone call or an email from a loved one asking for money urgently, always make sure to verify the story independently before you take any action.

Types of Scams

Foreign Lottery Scam

Calls or emails that claim you've won the Lottery or some other prize. They ask for a small fee or taxes to send your winnings.

- You will never win a contest of any kind if you did not enter it.
- Ignore all calls or emails claiming you've won
- NEVER share personal or banking information

"Congratulations! You may receive a certified check for up to $400,000,000 CASH
One Lump sum! Tax free!

SAY

If you ever receive a call or email saying you've won the lottery in a different country, then you've been the target of a foreign lottery scam.

- The call or email comes from some foreign lottery company notifying you that you have won a large amount of money.
- These emails usually look very professional with a subject line that congratulates you on winning the lottery and then the body of the email usually requests personal information like your full name, date of birth, or phone number.
- If it's a call, the person on the other end usually has a strong foreign accent to make it seem more legitimate.
- DO NOT provide any personal information.
- Remember, you can't win contests you didn't enter.

Types of Scams

Survey Scam

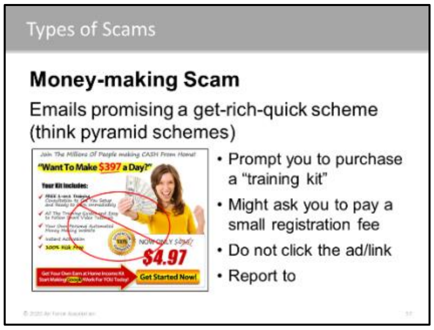
An email that prompts you to click on suspicious links to complete a survey for a prize

Do NOT click the link!

SAY

Survey scams are very common and usually come in the form of an email that prompts you to click on suspicious links to complete a survey and "win a prize." You might also receive a phone call from companies claiming to be giving away expensive trips or grand prizes for completing the survey.

- Don't click on the suspicious links.
- Don't give out any personal or financial information.
- Report the spam email or phone call to the relevant authority.



Types of Scams

Money-making Scam

Emails promising a get-rich-quick scheme (think pyramid schemes)

Join The Millions Of People making CASH From Home!
"Want To Make $397 a Day?"
Your Kit Includes:
NOW ONLY $4.97
Get Started Now!

- Prompt you to purchase a "training kit"
- Might ask you to pay a small registration fee
- Do not click the ad/link
- Report to

SAY

People love making a quick buck. Get-rich-quick scams promise that you can make some amount of money working from home and with minimum effort. Signs of a money-making scam include:

- A prompt to purchase a trial kit or training package for a fixed amount to be paid over PayPal or by sending them a check.
- Company is based overseas and provides little to no contact information.
- A deal that sounds too good to be true (because it's not true!).

If you think it's a scam, do a quick google search. You might find out that there's already some information online about the illegitimacy of the suspicious company.

Types of Scams

Tech Support Scam

Phony tech support calls or pop-ups claiming there's something wrong account/computer

- Gain remote access to the victim's computer
- Demand money to solve made-up issue
- Might install harmful malware

Tech-support will not contact you if you did not contact them first!

SAY

This very CyberGenerations program was created when the CyberPatriot Commissioner received a phone call from his mother regarding the legitimacy of a "Microsoft" tech support agent asking for her log-in information. As it turned out, that phone call was a tech support scam!

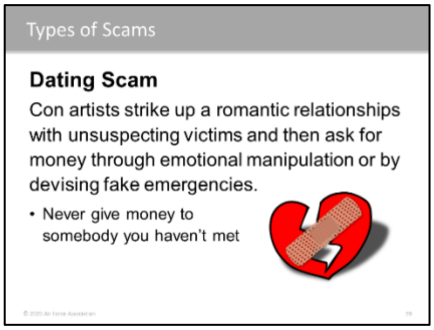
In tech support scams, bogus tech support employees make calls claiming to be from trusted companies like Microsoft or Apple.

- They tell you that they have detected a problem with your computer, and they need your login credentials to remotely access and fix the issue.
- Once they have access to the computer, the hacker might demand money, or they might install malware on the computer that helps them steal valuable personal data from the victim.

The on-screen pop-up or email version of this scam similarly warns you about security issues on your computer. It instructs you to dial a number for help or to click a link to download antivirus software. It might look like an error message from your operating system or like antivirus software.

- Do not call the number or click on the link!
- Do not assume that people contacting you are working for the company they say they are.

- Don't share personal or financial information.
- REMEMBER: Tech support will not contact you if you did not contact them first.



Types of Scams

Dating Scam

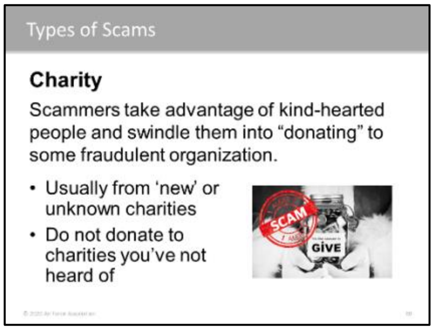
Con artists strike up a romantic relationships with unsuspecting victims and then ask for money through emotional manipulation or by devising fake emergencies.

- Never give money to somebody you haven't met

SAY

Scammers usually connect with their victims through some online dating site posing as interested singles looking to make a genuine connection with a like-minded individual.

- Be cautious of people who claim to be madly in love with you, even before they have met you in person.
- Beware of people who claim to be Americans working overseas, like soldiers.
- Even if you feel a strong connection, don't ever send money to someone you haven't met in-person.



Types of Scams

Charity

Scammers take advantage of kind-hearted people and swindle them into "donating" to some fraudulent organization.

- Usually from 'new' or unknown charities
- Do not donate to charities you've not heard of

ASK

Has anyone here ever donated money to a charity you weren't too familiar with, or maybe you've given to a door-to-door solicitor who claimed to be supporting a good cause?

SAY

Charity scams are usually very sophisticated, and many people fall prey to them on a regular basis. The scammers take advantage of kind-hearted people and swindle them into "donating" to bogus organizations.

- Whenever there's any natural disaster or ongoing humanitarian crisis, these scammers use high-pressure sales tactics to extract money from unsuspecting victims.
- Do your research before donating to any organization.
- Delete unsolicited emails and stick to organizations you know and trust.

Types of Scams

An attacker who secretly intercepts and possibly modifies messages between two parties

This slide links to an external resource.

SAY

Sometimes criminals will try to trick you into sharing sensitive information by luring you into a trap. This is usually done through a man-in-the-middle scam. Let's walk through AT&T's breakdown of how it works.

DO

Open the man in the middle slide show (click the image) and walk through the explanation.

Identity Theft

Identity Theft

Identity thieves defraud people and the government by assuming the identities of unsuspecting victims and using that to commit a wide range of illegal activities.

What to do in case of identity theft:

- Contact the organization where the theft occurred and alert them
- Contact a Credit Reporting Agency and ask them to place a fraud alert for your credit report
- Report identity theft to the FTC (www.IdentityTheft.gov)

This slide has 3 builds.

This slide links to an external resource.

SAY

Identity thieves defraud people and the government by assuming the identities of unsuspecting victims and using those stolen identities to commit a wide range of illegal activities.

- The increasing use of online tax filing services makes it even easier for scammers to steal your information and use it to make fraudulent tax claims.
- Scammers may also use the stolen information to submit fraudulent billings to Medicare or Medicaid or to receive other social security benefits.

ASK

Identity theft is a serious issue. What should you do if your identity gets stolen?

SAY

Build 1

- Contact the organization where the theft occurred and alert them.

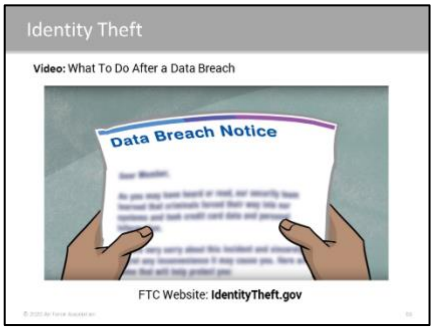
Build 2

- Contact a Credit Reporting Agency and ask them to place a fraud alert for your credit report.

Build 3

- Report identity theft to the FTC at IdentityTheft.gov

  Facilitator note: If you wish to show the class the FTC website, click the link on the slide.



Identity Theft

Video: What To Do After a Data Breach

FTC Website: **IdentityTheft.gov**

This slide links to an external resource.

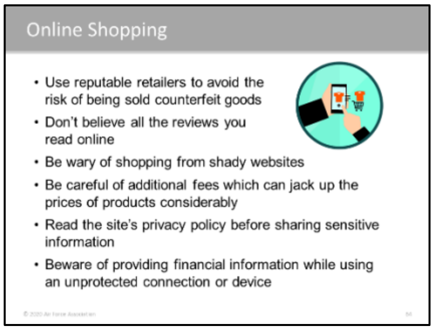
SAY

This video was created by the FTC. It discusses the basic steps to take to protect your identity after a data breach.

DO

Open the *What to do after a data breach* video (click the image).

Online Shopping



Online Shopping

- Use reputable retailers to avoid the risk of being sold counterfeit goods
- Don't believe all the reviews you read online
- Be wary of shopping from shady websites
- Be careful of additional fees which can jack up the prices of products considerably
- Read the site's privacy policy before sharing sensitive information
- Beware of providing financial information while using an unprotected connection or device

SAY

Online shopping is convenient, but it can also be risky if you aren't careful. Follow this advice for a positive and safe online shopping experience:

- If the price of a good is heavily reduced or the offer looks like it's too good to be true, make sure to research the third-party seller before making the purchase.
- Reviews can be bought and sold, and false reviews are everywhere. Be especially skeptical of reviews which look too generic.
- Some sham websites have offers which often seem too good to be true and that's because they are! Most of the times, these websites are trying to steal your information. So, always verify the legitimacy of a website.

- Always check the additional fees that may appear during the checkout process, like shipping and handling fees, taxes, etc. If you think that the costs don't add up, cancel the order right there.
- Watch out for policies pertaining to how the retailer plans on using your personal information.
- Beware of providing financial information while using an unprotected connection or device.

Facilitator Note: Optional review activities available. See Appendix A3 and A4

Topic 6: Social Media Safety & Awareness (45 min.)

Social Media Safety & Awareness

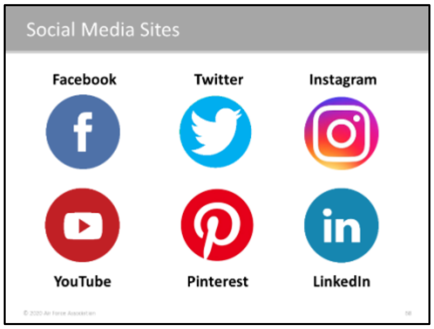
SAY

Social media has become an integral part of our daily lives. Social media has the ability to create connected communities made of people from across the globe.

- However, we must also acknowledge the dangers of using social media sites and the massive risks we are taking with our personal information when we use these sites.

In this section we will discuss some popular social media platforms, common social media scams, and some social media dos and don'ts.

Social Media Sites



Social Media Sites

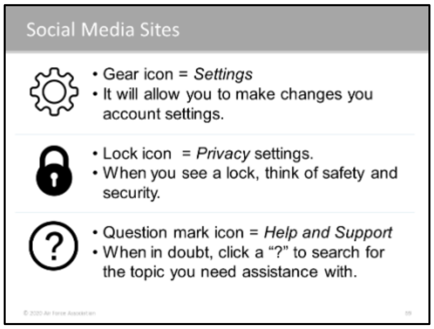
ASK

By a show of hands, how many people in here use one or more of these social media sites?

> *Facilitator note: You may follow up by asking individual participants what sites they use and how often they use them.*
>
> *If participants are not familiar with the functions of a particular site, use the explanations below:*

SAY

- Facebook is the most popular social media site among senior citizens, and is used to connect with friends and family and share updates/photos
- Twitter allows users to broadcast short messages (“tweets”) in 280 characters or less
- Instagram allows users and brands to share captioned photos
- YouTube is a video-sharing website
- Pinterest is a digital pin board where users save content that they find interesting (often fashion-, cooking-, crafting-, and home décor-related content)
- LinkedIn is a professional social media site that allows networking



Social Media Sites

- Gear icon = *Settings*
- It will allow you to make changes you account settings.

- Lock icon = *Privacy* settings.
- When you see a lock, think of safety and security.

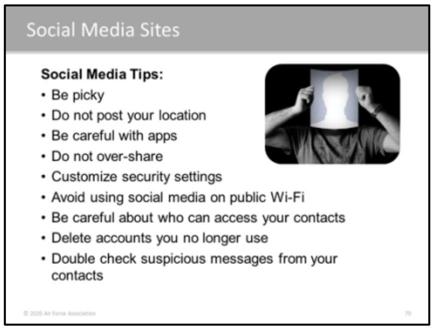
- Question mark icon = *Help and Support*
- When in doubt, click a “?” to search for the topic you need assistance with.

© 2020 Air Force Association 69

SAY

Securing your social media accounts is imperative to ensure a safe online experience.

- Every site has its own privacy settings, which are accessible typically under the “settings” option.
- When in doubt, search for “Privacy” and you will be able to navigate to the correct option which will let you make the desired changes.
- Remember, the icons for privacy settings may vary from site to site.



Social Media Sites

Social Media Tips:

- Be picky
- Do not post your location
- Be careful with apps
- Do not over-share
- Customize security settings
- Avoid using social media on public Wi-Fi
- Be careful about who can access your contacts
- Delete accounts you no longer use
- Double check suspicious messages from your contacts

© 2020 Air Force Association 70

This slide has 9 builds

SAY

There are many steps you can take to protect yourself from scams and information theft when using social media:

Build 1

- Be picky: Only “accept” or “follow” friends you know in real life.

Build 2

- Do not post your location: Friends who “tag” you may also be giving out your location.

Build 3

- Be careful with apps: Games like Candy Crush or location/geography tracking apps may give away your location or other identifiable information. They might also require you to download harmful content or adware. Never allow apps to store your log in credentials.

Build 4

- Don’t over-share: Just because a site asks for info, doesn't mean you have to give it. Try submitting a form with the least amount of information. If it does not go through, only fill out the required criteria. Oversharing also applies to the photos and events you share with your friends or the world.
  - If you wouldn't say it to someone's face, you shouldn't post it.

Build 5

- Customize your privacy settings: Do not use the default settings. They usually only provide the bare minimum in security. Be sure to update your settings regularly, too.

Build 6

- Avoid using social media on public networks: Public Wi-Fi is not secure, and you do not want to expose your login credentials over unsecure networks.

Build 7

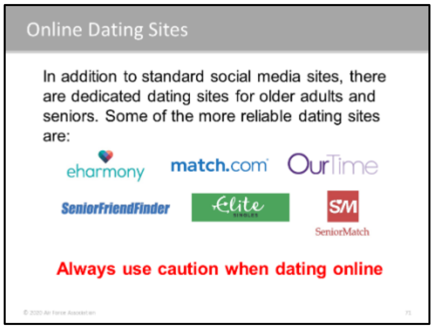
- Don’t share your contacts: If hackers get ahold of your contact list, they might send dangerous spam emails or messages with malicious content meant to harm them.

Build 8

- Delete accounts you no longer use: It’s best to delete online accounts which haven’t been used in a long time.

Build 9

- Do not reply to suspicious messages: Scammers can hack your friend’s account and send you a message trying to scam you. If you suspect that a certain message is fraudulent, directly contact the friend to verify the story.



Online Dating Sites

In addition to standard social media sites, there are dedicated dating sites for older adults and seniors. Some of the more reliable dating sites are:

Always use caution when dating online

71

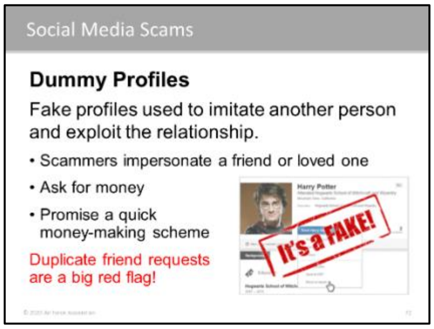
SAY

Just like social media sites, sites made specifically for online dating can be useful, but also dangerous. Some steps to consider with online dating are:

- Modify your online privacy settings to ensure that you only reveal what you want to reveal.
- Search for your date online to confirm identity.
- Check popular social media sites for the individual’s other profiles.
- Recognize red flags when something sounds too good to be true.

- Meet in a public place at first to confirm that they are who they say they are.

Social Media Scams



Social Media Scams

Dummy Profiles

Fake profiles used to imitate another person and exploit the relationship.

- Scammers impersonate a friend or loved one
- Ask for money
- Promise a quick money-making scheme

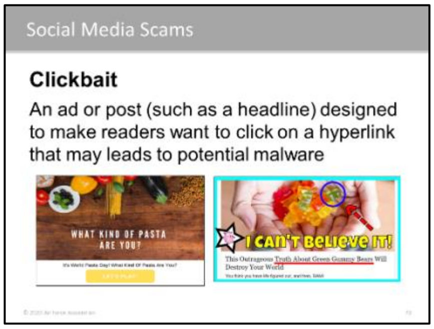
Duplicate friend requests are a big red flag!

SAY

Just like the internet, social media sites also have scams.

The biggest problem with sites like Facebook or Twitter is the use of dummy accounts. Dummy accounts are fake profiles that scammers use to imitate another person and exploit their relationships.

- Hackers can easily steal the information of your loved ones and reach out to you with some urgent financial emergency that requires you to make a wire transfer or they can lure you in with the promise of some brilliant business opportunity that will make you rich overnight.
- Be careful about any friend request from a person who you are already friends with on that particular platform. Duplicate friend requests are a big red flag.



Social Media Scams

Clickbait

An ad or post (such as a headline) designed to make readers want to click on a hyperlink that may leads to potential malware

WHAT KIND OF PASTA ARE YOU?

It's World Pasta Day! What Kind Of Pasta Are You?

I CAN'T BELIEVE IT!

This Outrageous Truth About Green Gummy Bears Will Destroy Your World

ASK

Take a moment to consider these two "articles." What do you think could happen if you open these links?

Facilitator note: If the participants can't see the small print, read the article titles aloud.

SAY

Clicking on such links can redirect you to a different website with suspicious content or it can initiate the download of dangerous malware onto your device. It's called "bait" because the subjects are tailored to grab your attention and prompt you to want to learn more immediately.

Social Media Scams

Sick Baby Hoax

Scammers use the real pictures of sick or disabled babies or children to manipulate people into donating money for emergency treatment.

- Don't like or share
- Report posts like these immediately
- Don't donate

SAY

A sick baby hoax is when scammers use real pictures of sick and disabled babies or young children to manipulate people into donating money for emergency treatment that will save their lives.

ASK

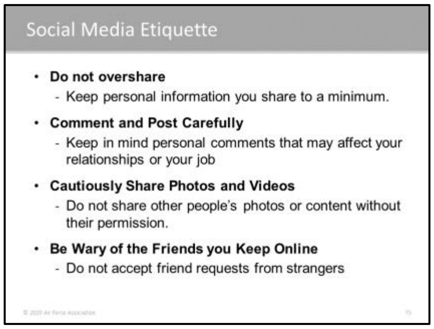
Be honest, has anyone ever shared such a post because you thought it was real?

SAY

People are often asked to like and share such photos to raise awareness, thereby making the hoax spread faster.

Families are often distressed to find that photos of their sick family member are being misused in this manner, but most of the times, there's very little they can do to stop the circulation of the post. So, you need to report such posts immediately. Obviously, you should never donate to such causes.

Social Media Etiquette



Social Media Etiquette

- **Do not overshare**
  - Keep personal information you share to a minimum.
- **Comment and Post Carefully**
  - Keep in mind personal comments that may affect your relationships or your job
- **Cautiously Share Photos and Videos**
  - Do not share other people's photos or content without their permission.
- **Be Wary of the Friends you Keep Online**
  - Do not accept friend requests from strangers

SAY

When using social media, always remember that minding your manners is not just for the dinner table! Online etiquette is important for a safe and positive online experience.

- Don't Overshare: Keep the personal information you share to a minimum.
  - Do not announce vacation details.
  - Do not share information about other people.
  - Do not share financial information or any sensitive data on social media.
- Comment and Post Carefully: Be careful with personal comments which may affect your relationships.
  - Consider how your comments may be perceived before posting them.

  - If you think that one of your friends might be interested in a post, send them a message directly rather than tagging them in the post.
  - When posting online, try not to flood people's feeds. Post responsibly.
- Cautiously Share Photos and Videos: Do not repost someone else's photos, media, or any other kind of content without their permission.
  - Ask before you post pictures of other people.
- Be Wary of the Friends You Keep: It's best to invite and accept friend requests from people you know.
  - Cybercriminals try to gain your personal information by sending false friend requests.

Topic 7: Jeopardy Review (30 min.)

Jeopardy Review

Congratulations! You've made it to the end of the CyberGenerations workshop. To test how much you've learned, we're going to play a game you're probably all familiar with…

Activity: Program Review

It's time to play…

JEOPARDY!

The game you know and love!

© 2020 Air Force Association

77

This slide requires an external resource.

DO

Open CyberGenerations_Jeopardy.ppt file.

Facilitator notes:

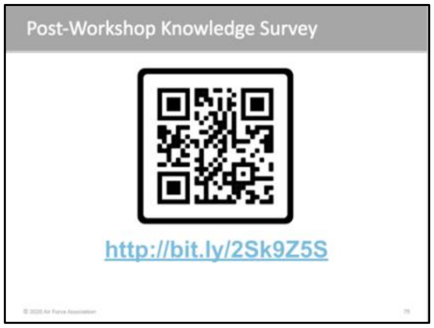
- *Supplies: CyberGenerations_Jeopardy.ppt, pen/paper for Final Jeopardy round, prizes for winners (optional)*
- *Teams: The game can be played individually or in small teams of 2-3 players.*
- *Scoring: Award question point amount for correct response. Subtract point amount for incorrect response. Instructor should keep track of points or assign a point tracker. Team with the most points (or dollar amount) at the end of Final Jeopardy wins.*
- *Directions:*

  - *Instructions for use of Jeopardy PowerPoint found on first slide.*
  - *Game intro slide begins on slide 2. Click through to introduce Categories until you reach the main playing board*

  Sound effects are available, as well as 'silent' option to stop any sound.

- *To Play:*
  - *Each player/team will take turns picking a category and amount.*
  - *Read question, then click Start Timer (5 seconds). Team must answer within time limit.*
  - *Click 'Go to Answer (question)' to view correct answer.*
  - *Click house icon to return to the main board.*
- *Daily Double:*
  - *Player/team will wager an amount. If answered correctly, they earn the wagered amount. If answered incorrectly, they lose the wagered amount.*
- *Final Jeopardy (hand out paper and pen to each team):*
  - *Each player/team wager an amount before the question is presented.*
  - *Once wagers are in, present questions and play 'timer' sound effect.*
  - *All teams write their answer on a piece of paper before time runs out.*
  - *At the end of the timer they will reveal their answers.*

Topic 8: Post-Workshop Survey (5 min.)



Post-Workshop Knowledge Survey

http://bit.ly/2Sk9Z5S

© 2020 Air Force Association

79

SAY

Now that you've gone through CyberGenerations, it's time to complete the post-workshop knowledge survey. The changes in your knowledge level will be used to make improvements to the program, so it is important that you answer honestly and thoughtfully.

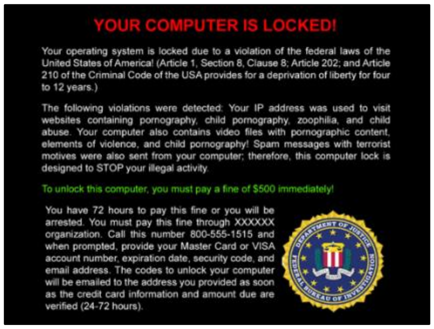
> *Facilitator Note: This is the same survey as the pre-workshop survey. Consider providing a few laptops for attendees to use to complete the survey. Attendees with smartphones may complete the survey on their devices by scanning the QR code with their phone cameras or using the URL.*

Appendix A: Supplemental Activities

Facilitator notes: These activities are optional. For the activities in this section,

- Divide the participants into smaller groups of 3 or 4 people.
- *Allow 5-7 minutes for groups to come up with their responses.*
- *Suggestion slides are not an exhaustive list of correct answers, but merely a guide.*

A1: Scenario 1 / Suggestions



YOUR COMPUTER IS LOCKED!

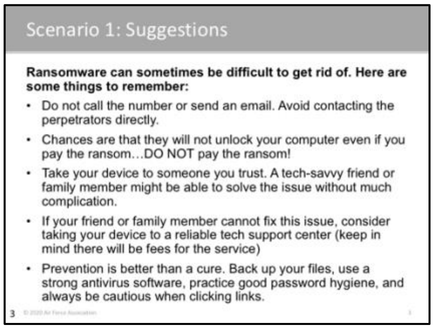
Your operating system is locked due to a violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; and Article 210 of the Criminal Code of the USA provides for a deprivation of liberty for four to 12 years.)

The following violations were detected: Your IP address was used to visit websites containing pornography, child pornography, zoophilia, and child abuse. Your computer also contains video files with pornographic content, elements of violence, and child pornography! Spam messages with terrorist motives were also sent from your computer; therefore, this computer lock is designed to STOP your illegal activity.

To unlock this computer, you must pay a fine of $500 immediately!

You have 72 hours to pay this fine or you will be arrested. You must pay this fine through XXXXXX organization. Call this number 800-555-1515 and when prompted, provide your Master Card or VISA account number, expiration date, security code, and email address. The codes to unlock your computer will be emailed to the address you provided as soon as the credit card information and amount due are verified (24-72 hours).

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION



Scenario 1: Suggestions

Ransomware can sometimes be difficult to get rid of. Here are some things to remember:

- Do not call the number or send an email. Avoid contacting the perpetrators directly.
- Chances are that they will not unlock your computer even if you pay the ransom…DO NOT pay the ransom!
- Take your device to someone you trust. A tech-savvy friend or family member might be able to solve the issue without much complication.
- If your friend or family member cannot fix this issue, consider taking your device to a reliable tech support center (keep in mind there will be fees for the service)
- Prevention is better than a cure. Back up your files, use a strong antivirus software, practice good password hygiene, and always be cautious when clicking links.

3 © 2020 Air Force Association

DO

Read the scenario aloud.

Build 1

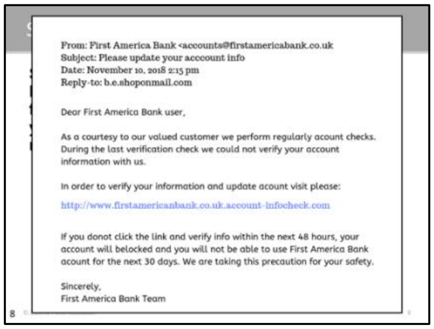
SAY

Read this message carefully and then work with your assigned group to come up with some suggestions for the steps you can take to secure your information.

DO

Review Scenario 1 Suggestion slide once groups have presented their answers.

A2: Scenario 2



From: First America Bank <accounts@firstamericabank.co.uk
Subject: Please update your acccount info
Date: November 10, 2018 2:15 pm
Reply-to: b.e.shoponmail.com

Dear First America Bank user,

As a courtesy to our valued customer we perform regularly acount checks. During the last verification check we could not verify your account information with us.

In order to verify your information and update acount visit please:

http://www.firstamericanbank.co.uk.account-infocheck.com

If you donot click the link and verify info within the next 48 hours, your account will belocked and you will not be able to use First America Bank acount for the next 30 days. We are taking this precaution for your safety.

Sincerely,
First America Bank Team

8

DO

Read the scenario aloud.

Build 1

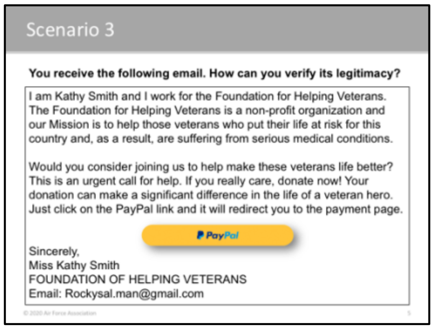
SAY

Read this email carefully and then work with your assigned group to find all the red flags. You should also try and come up with some suggestions for how you can verify the authenticity of this email.

DO

Review answers as a class.

A3: Scenario 3 / Suggestions



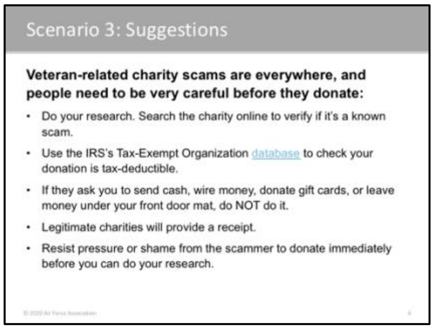
Scenario 3

You receive the following email. How can you verify its legitimacy?

I am Kathy Smith and I work for the Foundation for Helping Veterans. The Foundation for Helping Veterans is a non-profit organization and our Mission is to help those veterans who put their life at risk for this country and, as a result, are suffering from serious medical conditions.

Would you consider joining us to help make these veterans life better? This is an urgent call for help. If you really care, donate now! Your donation can make a significant difference in the life of a veteran hero. Just click on the PayPal link and it will redirect you to the payment page.

Sincerely,
Miss Kathy Smith
FOUNDATION OF HELPING VETERANS
Email: Rockysal.man@gmail.com



Scenario 3: Suggestions

Veteran-related charity scams are everywhere, and people need to be very careful before they donate:

- Do your research. Search the charity online to verify if it's a known scam.
- Use the IRS's Tax-Exempt Organization database to check your donation is tax-deductible.
- If they ask you to send cash, wire money, donate gift cards, or leave money under your front door mat, do NOT do it.
- Legitimate charities will provide a receipt.
- Resist pressure or shame from the scammer to donate immediately before you can do your research.

DO

Read the scenario aloud

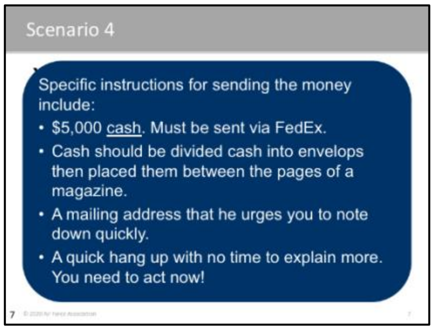
SAY

Work with your assigned group to find all the red flags. You should also try and come up with some suggestions for how you can verify the authenticity of this email.

DO

- Review Scenario 3 Suggestion slide once groups have presented their answers.
- If time permits, visit the FTC link to go over the suggestions in details:
  - https://www.consumer.ftc.gov/articles/giving-charities-help-veterans

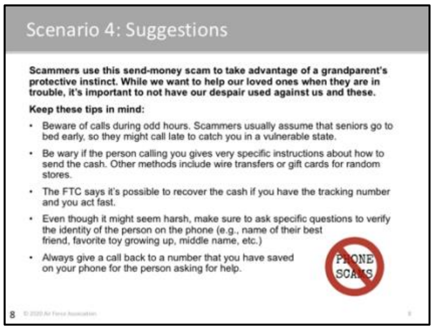
A4: Scenario 4 / Suggestions



Scenario 4

Specific instructions for sending the money include:

- $5,000 cash. Must be sent via FedEx.
- Cash should be divided cash into envelops then placed them between the pages of a magazine.
- A mailing address that he urges you to note down quickly.
- A quick hang up with no time to explain more. You need to act now!



Scenario 4: Suggestions

Scammers use this send-money scam to take advantage of a grandparent's protective instinct. While we want to help our loved ones when they are in trouble, it's important to not have our despair used against us and these.

Keep these tips in mind:

- Beware of calls during odd hours. Scammers usually assume that seniors go to bed early, so they might call late to catch you in a vulnerable state.
- Be wary if the person calling you gives very specific instructions about how to send the cash. Other methods include wire transfers or gift cards for random stores.
- The FTC says it's possible to recover the cash if you have the tracking number and you act fast.
- Even though it might seem harsh, make sure to ask specific questions to verify the identity of the person on the phone (e.g., name of their best friend, favorite toy growing up, middle name, etc.)
- Always give a call back to a number that you have saved on your phone for the person asking for help.

DO

Read the scenario aloud.

Build 1

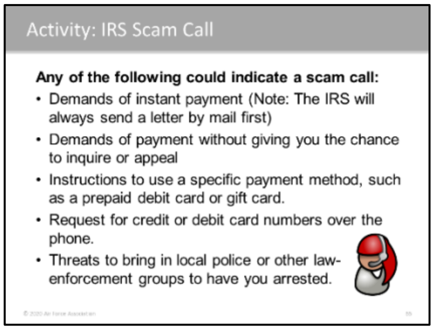
SAY

Read this situation carefully and then work with your assigned group to come up with some suggestions for the steps you must take if you find yourself in this position. What are the red flags?

DO

Review Scenario 4 Suggestion slide once groups have presented their answers.

A5: IRS Scam Call

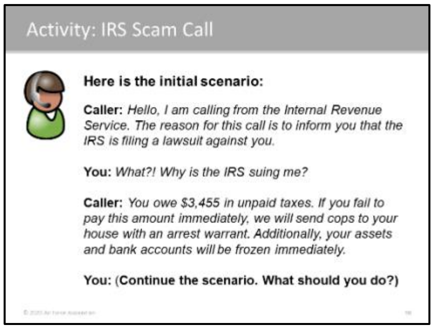


Activity: IRS Scam Call

Any of the following could indicate a scam call:

- Demands of instant payment (Note: The IRS will always send a letter by mail first)
- Demands of payment without giving you the chance to inquire or appeal
- Instructions to use a specific payment method, such as a prepaid debit card or gift card.
- Request for credit or debit card numbers over the phone.
- Threats to bring in local police or other law-enforcement groups to have you arrested.

© 2020 Air Force Association 55



Activity: IRS Scam Call

Here is the initial scenario:

Caller: *Hello, I am calling from the Internal Revenue Service. The reason for this call is to inform you that the IRS is filing a lawsuit against you.*

You: *What?! Why is the IRS suing me?*

Caller: *You owe $3,455 in unpaid taxes. If you fail to pay this amount immediately, we will send cops to your house with an arrest warrant. Additionally, your assets and bank accounts will be frozen immediately.*

You: (Continue the scenario. What should you do?)

© 2020 Air Force Association 56

Facilitator Note: You will need two participants to play out the scenario. Alternately, the instructor can also play the role of the scammer making the call.

This activity takes 10 minutes

SAY

This role-playing game provides you with an example of a fraudulent call from the IRS demanding money and threatening with dire consequences if you fail to pay immediately. According to the IRS, any one of the following factors indicates a scam:

- A call demanding instant payment. In fact, the IRS will not call about taxes payable without first sending you a bill by mail.
- A call demanding that you pay taxes without giving you the chance to enquire or appeal the amount they say you owe.
- Instructions to use a specific payment method, such as a prepaid debit card.
- A call asking for credit or debit card numbers over the phone.
- Threats to bring in local police or other law-enforcement groups to have you arrested.

Remember these tips when doing the role-playing scenario.

Next Slide

SAY

This is the script. We have only provided the initial scenario. The participant playing the scammer will begin with the dialogue in the script. After the initial scenario is played out, you must continue the conversation.

Facilitator note: This scenario can be played out a few different times with different participants, depending on the time left for the activity.

Appendix B: Facilitator Resources

B1: Facilitator Feedback Survey

Thank you for facilitating a CyberGenerations workshop! We truly appreciate your hard work and dedication to the CyberGenerations initiative. Your feedback is valuable to the continuous improvement of the program. We kindly ask that you please complete the survey in the link below:

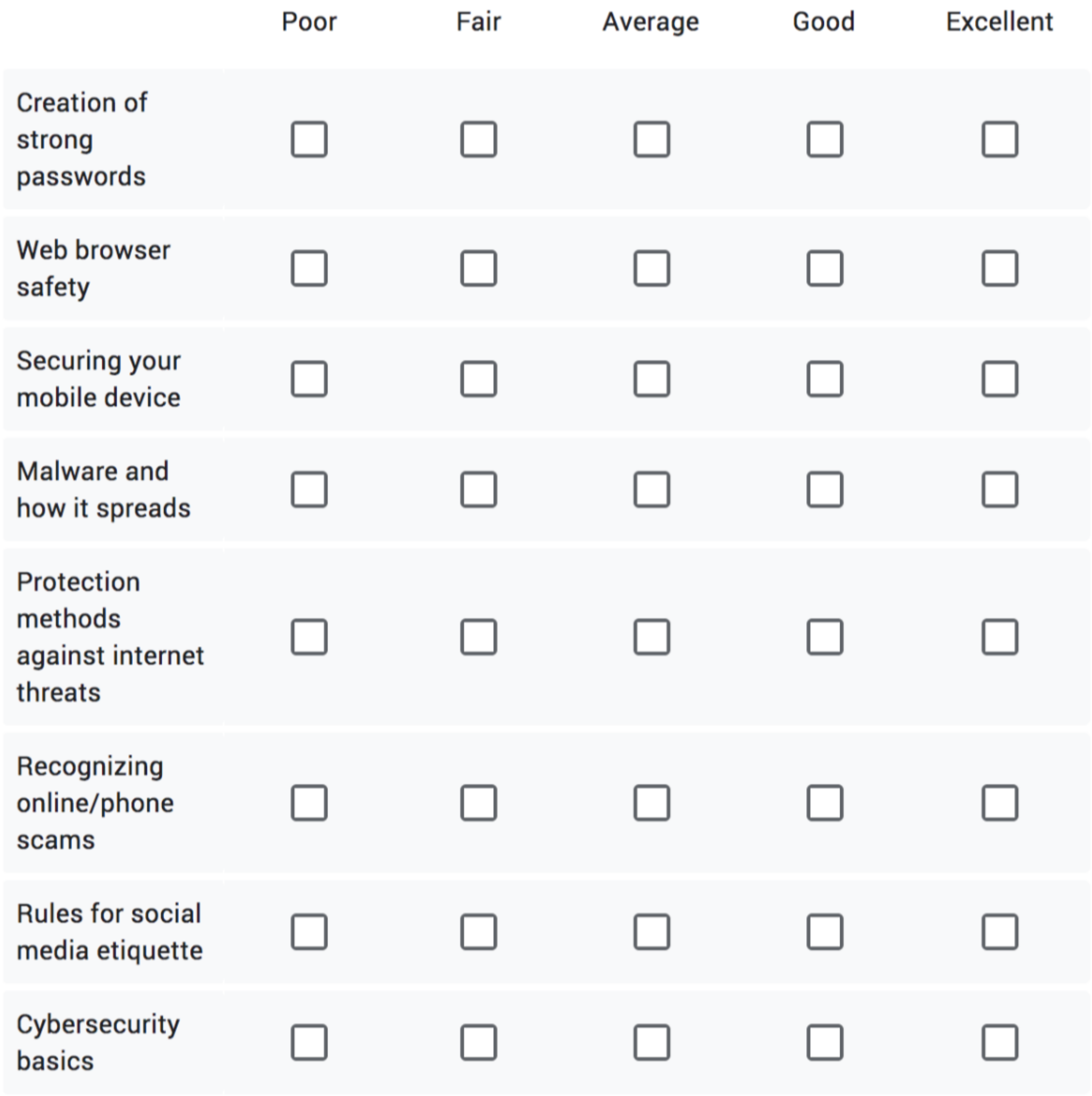
http://bit.ly/2SiQxWN

B2: CyberGenerations Knowledge Survey (Pre- and Post-Workshop)

The purpose of this survey is to gauge your understanding of basic cybersecurity subjects both before AND after your participation in CyberGenerations. Through the questions below, please indicate when you are taking this survey and your perceived level of understanding for each of the listed subjects. Your feedback will be used to measure the success of the program and to make adjustments to future content as needed.

1. **I am completing this survey BEFORE / AFTER (circle option) participating in CyberGenerations.**

2. **Rate your knowledge of the following subjects, using the scale poor (no knowledge) to excellent (full knowledge). Check one rating per subject.**



	Poor	Fair	Average	Good	Excellent
Creation of strong passwords	□	□	□	□	□
Web browser safety	□	□	□	□	□
Securing your mobile device	□	□	□	□	□
Malware and how it spreads	□	□	□	□	□
Protection methods against internet threats	□	□	□	□	□
Recognizing online/phone scams	□	□	□	□	□
Rules for social media etiquette	□	□	□	□	□
Cybersecurity basics	□	□	□	□	□

CyberPatriot is the Air Force Association's
National Youth Cyber Education Program

For additional information visit www.uscyberpatriot.org

CyberGenerations is available through the generous support of:

AT&T